

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

<hr/>	X	
In re SONY BMG CD TECHNOLOGIES	:	Civil Action No. 1:05-cv-09575-NRB
LITIGATION	:	
<hr/>	:	<u>CLASS ACTION</u>
	:	
This Document Relates To:	:	DECLARATION OF LARRY PONEMON IN
	:	SUPPORT OF THE RICCIUTI CLASS
ALL ACTIONS.	:	REPRESENTATIVES' MEMORANDUM OF
<hr/>	X	LAW IN SUPPORT OF MOTION FOR AN
		AWARD OF ATTORNEYS' FEES AND
		REIMBURSEMENT OF EXPENSES

I, LARRY PONEMON, declare as follows:

1. I am the chairman and founder of Ponemon Institute, a “think tank” dedicated to advancing responsible information and privacy management practices in business and government. The Ponemon Institute conducts independent research, educates leaders from the private and public sectors, and verifies the privacy and data protection practices of organizations. Attached hereto as Exhibit A is a true and correct copy of my résumé. I have personal knowledge of the matters stated herein and, if called upon, I could and would competently testify thereto.

2. I am considered a leading international expert on privacy auditing and responsible information management. I have extensive experience in auditing self-regulatory frameworks for data protection and privacy compliance in the United States, Canada, the European Union, Hong Kong and other nations.

3. I was appointed to the Advisory Committee on online privacy and security by the United States Federal Trade Commission. I also serve on various state privacy commissions including the California State Privacy Task Force and other initiatives.

4. I was asked to provide an estimate of the potential cost impact that Web-users may have experienced as a result of Sony BMG’s download of digital rights management (DRM) software products known as XCP or Media Max 5.0.<sup>1</sup> For purposes of my analysis, these two software technologies are referred to as spyware because the Web-user was unlikely to know, control or uninstall these software products, and they create the opportunity for the user’s desktop or laptop computer to suffer malfunctions including security threats.

---

<sup>1</sup> MediaMax 3.0 was omitted from my analysis because this DRM software product does not appear to open a door to potential malfunctions or security threats.

5. My analysis of the spyware cost impact for consumers is based on sample research findings from a national study released in May 2005.<sup>2</sup> Research methods in this study utilized a survey instrument. Adult-aged individuals throughout the United States provided information about their spyware experience.

6. One set of survey questions dealt with the monetary cost and time-related effort associated with respondents' spyware experience. The research did not attempt to collect proof of expenses or other pieces of evidence concerning each individual's time-related efforts. All responses were self-reported within the survey instrument.

7. I believe that there are inherent limitations to survey research that need to be carefully considered before drawing inferences from sample findings to the present case. The following items are specific limitations that are germane to most perception-capture surveys:

(a) Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying experience or beliefs than those who completed the instrument.

(b) Sampling bias: Because sampling frames were derived from mail lists, the quality of results is influenced by the accuracy of contact information and the degree to which the list is representative of individuals who are informed about current events. We also acknowledge that the results may be biased by media coverage at the time of the study.

---

<sup>2</sup> National Spyware Study, Ponemon Institute Report, May 17, 2005. A true and correct copy of this study is attached hereto as Exhibit B.

(c) Self-report bias: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that subjects did not adequately describe their beliefs or perceptions regarding spyware.

8. The sample of results reference 1,630 respondents – all of whom indicating that they experienced some form of spyware infection (including adware and malware) on their computer sometime over a 12 month time period.<sup>3</sup>

Has spyware on your desktop or laptop caused you to suffer a monetary loss, a productivity loss or inconvenience?	Frequency	Total Percentage
Yes	1,401	86%
No	229	14%
Total	1,630	100%

9. The analysis shows that 1,401 respondents (86%) stated that spyware has caused them to suffer a monetary loss, a productivity loss or inconvenience. A second analysis required these 1,401 respondents to list their nature of negative experiences.

10. The following table provides a distribution of responses in ascending order of importance based on the frequency of responses. Please note that the percentage of total responses sums to more than 100% because respondents could check more than one item. The largest negative impact (87%) concerns the respondents' lost productivity as a result of spyware infection. The second most significant impact (34%) concerns respondents' inability to use previously downloaded software as a result of spyware infection.

---

<sup>3</sup> In this study, 87% of respondents said that they *do not read* the End User License Agreement or EULA prior to downloading software.

What best describes this negative impact? (Check all that apply.)	Frequency	Total Percentage
Experienced productivity losses.	1,214	87%
Could not use previously downloaded software.	475	34%
Purchased anti-spyware or anti-virus software.	371	26%
Hired a computer pro to fix my desktop or laptop.	200	14%
Purchased additional protection services from my ISP or DSL provider.	128	9%
Leakage of my personal information without consent or knowledge.	51	4%
Replaced my computer with new hardware.	28	2%
Monetary damages resulting from criminal activity or related abuses.	10	1%

11. The third analysis asked respondents to state an approximate monetary or out-of-pocket cost impact incurred over the past year. They were also given an opportunity to state “no monetary loss.” In total, 205 respondents (15%) report a monetary loss as a result of spyware. The remaining 1,190 (85%) did not report a monetary loss.

12. For the 205 respondents who report a monetary loss, I extrapolated an average cost burden based on the median value for each one of six cost categories in the instrument (shown below).

13. For the highest cost category (over \$200), I utilized a conservative median value of \$220 (or 110% the category minimum).

Approximately, what is the monetary or out-of-pocket loss over the past 12 months as a result of having spyware on your computer? Please check the range that is closest to the total loss experienced.	Frequency	Total Percentage	Median Cost in Range	Calculation
No Monetary Loss	1,190	85%	-	-
Between \$0 and \$10	23	2%	5	0.1
Between \$10 and \$20	66	5%	15	0.7
Between \$20 and \$50	60	4%	35	1.5
Between \$50 and \$100	31	2%	75	1.7
Between \$100 and \$200	12	1%	50	1.3
Over \$200	13	1%	220	2.1
Total	1,395	100%	Average	7.3
Number of people with self-reported monetary loss	205	15%		

14. The summation of all median values multiplied by the percentage frequency of responses in each cost category is the basis of a \$7.3 point estimate for an overall monetary cost impact. This extrapolated cost burden is a value that applies to all 1,395 respondents, and not just those 205 people (15%) that reported a monetary loss. Hence, the extrapolated per capital cost is \$1.07 (defined as \$7.3 multiplied by 15%).

15. The fourth analysis asked respondents to state an approximate time impact incurred over the past year. They were also given an opportunity to state “no time” loss. A total of 1,066 respondents (76%) report time losses as a result of spyware. The remaining 336 (24%) did not report a time loss.

16. For the 1,066 respondents who report a time loss, we extrapolate an average time burden based on the median value for each one of six time range categories in the instrument (shown below). For the highest time category (over 100 hours), we utilized a conservative median value of 120 hours (or 120% the category minimum).

Approximately, how much time did you spend over the past 12 months as a result of having to deal with spyware on your computer? Please check the range that is closet to the total time spent by you.	Frequency	Percentage	Average Time Percentage	Calculation
No time	336	24.0%	-	-
Between 0 and 60 minutes	899	64.1%	0.5	0.32
Between 1 to 5 hours	123	8.8%	2.5	0.22
Between 5 to 10 hours	19	1.4%	7.5	0.10
Between 10 to 50 hours	15	1.1%	30.0	0.32
Between 50 to 100 hours	7	0.5%	75.0	0.37
Over 100 hours	3	0.2%	120.0	0.26
Total	1,402	100.0%	Average	1.59
Number of people who self-reported time loss	1,066	76.0%		

17. The summation of all median values multiplied by the percentage frequency of responses in each time category is the basis of a 1.59 hour point estimate for an overall time impact. This extrapolated time burden is a value that applies to all 1,402 respondents, and not just those 1,066 people (76%) that reported a time loss. Hence, the extrapolated per capital time burden is 1.21 hours (defined as 1.59 hours multiplied by 76%).

18. For purposes of a very conservative estimate for the value of lost time in responding to spyware infection on a desktop or laptop computer, I used the US minimum wage as of March 1, 2006 at \$5.15 per hour. Assuming this hourly pay rate, the average extrapolated time-related cost impact of spyware is \$6.24 (defined as 1.21 hours multiplied by \$5.15 minimum wage hourly rate).

19. Drawing upon the above calculated values derived from sample data, I made the following inferences about the total cost impact on Web users that downloaded XCP and Media Max 5.0. Please note that I am basing this analysis on the following factors:

(a) Sample results can be used to approximate the two plaintiff classes with respect to the end-user spyware experience.

(b) XCP and Media Max 5.0 unleash spyware, causing approximately the same potential for malfunction and security threats for the end-user.

(c) One year, on average, is the approximate time impact for an individual in one of the two plaintiff classes.

(d) The approximate plaintiff class totals for XCP and Media Max 5.0 are 3 million and 4.2 million people, respectively.

(e) Of all CD purchasers, I assume that approximately 20% actually loaded their CDs onto their desktop or laptop computers. Hence, the number of XCP users that experienced a spyware infection is estimated at 600,000 individuals (3 million CD purchasers multiplied by 20%). The number of Media Max 5.0 users that experienced spyware is estimated at 840,000 individuals (4.2 million CD purchasers multiplied by 20%).

20. The following table reports the extrapolated total cost impact (expressed in U.S. million dollars) for two plaintiff classes:

SONY BMG DRM software categories	Million Web users	Monetary cost (\$Million)	Time cost (\$Million)	Estimated Cost Impact (\$Million)
XCP	0.60	0.64	3.74	4.39
Media Max 5.0	0.84	0.90	5.24	6.14
Total	1.44	1.54	8.99	10.53



21. Assuming that the average U.S. wage rate published by the Department of Labor Statistics on March 30, 2006 is used instead of the minimum wage, the total estimated time cost would be \$32.76 million dollars, and the total estimated cost impact would be \$34.30 million dollars. These figures are based on an average reported weekly wage of \$751 dollars and an assumed 40 hour average work week.

I declare under penalty of perjury under that the foregoing is true and correct. Executed this 6th day of April, 2006, at Elk Rapids, Michigan.



---

LARRY PONEMON